What is claimed is:

1. A security management system for controlling a security status of each of a plurality of managed systems constituting an information system in accordance with an information security policy representing a policy of a security measure, comprising:

a plurality of management sections corresponding to at least one managed system and the information security policy, each management section being for controlling the security status of the managed system corresponding thereto so as to adjust the security status to the information security policy corresponding thereto;

a database registering a correspondence of the information security policy, the managed system and each management section;

a security content reception section for receiving a selection of a range of the information security policy and the managed system from a user;

an extraction section for extracting from said database the management section registered so as to correspond to the information security policy and the

managed system included in the range in which said security content reception section has received the selection; and

a management control section for allowing the management section extracted by said extraction section to change the security status of the managed system corresponding to the management section so as to adjust to the information security policy corresponding to the management section.

2. A security management system for auditing a security status of each of a plurality of managed systems constituting an information system, the security status concerning an information security policy representing a policy of a security measure, comprising:

a plurality of audit sections corresponding to at least one managed system and at least one information security policy, each audit section being for auditing the security status concerning the corresponding information security policy of the corresponding managed system;

a database registering a correspondence of the information security policy, the managed system and the audit section;

a security content reception section for

receiving a selection of a range of the information security policy and the managed system from the user;

an extraction section for extracting from said database the audit section registered so as to correspond to the information security policy and the managed system included in the range in which said security content reception section has received the selection; and

an audit control section for allowing the audit section extracted by said extraction section to audit the security status concerning the information security policy of the managed system corresponding to the audit section.

3. A security management system for controlling a security status of each of a plurality of managed systems constituting an information system in accordance with an information security policy representing a policy of a security measure, comprising:

a plurality of management sections corresponding to at least one managed system and at least one information security policy, each management section being for controlling the security status of the corresponding managed system so as to adjust the security state to the corresponding information

security policy;

a plurality of audit sections corresponding to at least one managed system and at least one information security policy, each audit section being for auditing the security status concerning the corresponding information security policy of the corresponding managed system;

a database registering a correspondence of the information security policy, the managed system, the management section and the audit section;

a security content reception section for receiving a selection of a range of the information security policy and the managed system from a user;

an extraction section for extracting from said database the management section and the audit section, which are registered so as to correspond to the information security policy and the managed system included in the range in which said security content reception section has received the selection;

a management control section for allowing the management section extracted by said extraction section to change the security status of the managed system corresponding to the management section so as to adjust to the information security policy corresponding to the management section; and

an audit control section for allowing the audit

section extracted by said extraction section to audit the security status concerning the information security policy of the managed system corresponding to said audit section.

4. A security management method for controlling a security status of each of a plurality of managed systems constituting an information system with an electronic computer in accordance with an information security policy representing a policy of a security measure, comprising the steps of:

receiving a selection of a range of the information security policy and the managed system from a user;

extracting a management program corresponding to an information security policy and a managed system, included in the range in which the selection has been received, among a plurality of management programs describing a processing for controlling the security status of the corresponding managed system so as to adjust the security status to the corresponding information security policy, the plurality of management programs corresponding to at least one information security policy and at least one managed system, which are previously stored; and

allowing the electronic computer to execute the

extracted management program and to change the security status of the managed system corresponding to the management program so that the security status thereof is adjusted to the information security policy corresponding to the management program.

5. A security management method for auditing, with an electronic computer, a security status of each of a plurality of managed systems constituting an information system, the security status concerning an information security policy representing a policy of a security measure, comprising the steps of:

receiving a range of a selection of the information security policy and the managed system from a user;

extracting an audit program registered so as to correspond to the information security policy and the managed system, which are included in the range in which the selection has been received, among a plurality of audit programs describing a processing for auditing the security status concerning the corresponding information security policy of the corresponding managed system, the plurality of audit programs corresponding to at least one information security policy and at least one managed system, which are previously stored; and

allowing the electronic computer to execute the extracted audit program and to audit the security status of the managed system corresponding to the audit program, the security status concerning the information security policy corresponding to the audit program.

6. A storage medium storing a program for controlling a security status of each of a plurality of managed systems constituting an information system in accordance with an information security policy representing a policy of a security measure,

wherein said program is read out and executed by an electronic computer,

to construct, on said electronic computer,

a security content reception section for receiving a selection of a range of the information security policy and the managed system from a user;

an extraction section for extracting a management program corresponding to an information security policy and a managed system, which are included in the range in which said security content reception section has received the selection, from a database storing a plurality of management programs describing a processing for controlling the security status of the corresponding managed system so as to adjust the

security status of the managed system to the corresponding information security policy, the plurality of management programs corresponding at least one managed system and at least one information security policy; and

a management control section for allowing said electronic computer to execute the management program executed by said extraction section and to change the security status of the managed system corresponding to the extracted management program so as to adjust the security status to the information security policy corresponding to the extracted management program.

7. A storage medium storing a program for auditing a security status concerning an information security policy representing a policy of a security measure of a plurality of managed systems constituting an information system,

wherein said program is read out and executed by an electronic computer,

to construct, on said electronic computer,

a security content reception section for receiving a selection of a range of the information security policy and the managed system from a user;

an extraction section for extracting an audit program registered so as to correspond to an

information security policy and a managed system, which are included in the range in which said security content reception section has received the selection, from a database storing a plurality of audit programs describing a processing for auditing the security status concerning the corresponding information security policy of the corresponding managed system, the plurality of audit programs corresponding to at least one managed system and at least one information security policy; and

an audit control section for allowing the electronic computer to execute the audit program extracted by said extraction section and to audit the security status concerning the information security policy corresponding to the audit program of the managed system corresponding to the audit program.

8. A security management method for supporting a security management of each of a plurality of managed systems constituting an information system with an electronic computer, comprising:

a security specification hatching step of extracting an information security policy made to correspond to each managed system constituting an information system designated by a user from a database describing a correspondence of an information security

policy representing a policy of a security measure with at least one managed system, to hatch security specifications to be applied to the information system;

a security diagnosis step of executing a plurality of audit programs describing a processing for auditing various information including a type of the managed system and a software version, which are stored so as to correspond to each set of the information security policy and the managed system, the information security policy and the managed system being specified by security specifications hatched in said security specification hatching step, as well as a security status concerning the information security policy of the managed system, to audit the various information including the type and the software version of the managed system constituting the information system designated by the user, and to diagnose a security of said information system; and

a security handling and management step of executing a management program designated by the user, among a plurality of management programs describing a processing for controlling the security status concerning the information security policy of the managed system stored so as to correspond to each set of the information security policy and the managed

system, which are specified by the security specifications hatched in said security specification hatching steps, to allow said electronic computer to change the security status of the managed system corresponding to the management program so as to adjust the security status to the information security policy corresponding to the management program.

9. The security management method according to claim 8,

wherein, in said security diagnosis step, the audit program made to correspond to each set of the information security policy and the managed system, which are specified by the security specifications hatched in said security specification hatching step, is extracted from a database describing a correspondence of the information security policy, the managed system and the audit program describing a processing for auditing various information such as a type and a software version of said managed system as well as the security status concerning said information security policy of said managed system, and executed, to diagnose the security of the information system designated by said user; and

in said security handling and management step, the management programs made to correspond to each set

of the information security policy and the managed system, which are specified by the security specifications hatched in said security specification hatching step, are extracted from a database describing a correspondence of the information security policy, the managed system and the management program describing a processing for controlling the security status concerning the security policy, the managed system and said information security policy of a security of said managed system, and the management program designated by the user is extracted among the extracted programs to be executed, to allow the security status of the managed system corresponding to the extracted management program to adjust to the information security policy corresponding to the management program.

10. The security management method according to claim 8,

wherein said security diagnose step is executed periodically.

11. The security management method according to claim 8,

wherein, in accordance with a setting content received from the user, said management program

changes the security status of the managed system corresponding to the management program so as to adjust the security status to the information security policy corresponding to the management program.

12. The security management method according to claim 8,

wherein a security hole information published by a security information organization including CERT or Computer Emergency Response Team and diagnosis results obtained in said security diagnose step which is executed for the information system designated by the user are reflected in the database describing the correspondence of the information security policy with at least one managed system and an audit/management program stored so as to correspond to each set of the information security policy and the managed system.

13. A security management system for supporting a security management of managed systems constituting an information system, comprising:

a database describing a correspondence of an information security policy representing a policy of a security measure with at least one managed system;

a security specification hatching section for extracting an information security policy made to

correspond to each of the managed systems constituting the information system designated by a user from said database, to hatch security specifications to be applied to the information system;

a plurality of audit sections for auditing various information including a type and a software version of the managed system as well as a security status concerning the information security policy of the managed system, each audit section being provided so as to correspond to each set of the information security policy and the managed system, which are specified by security specifications hatched by said security specification hatching section, and;

a security diagnosis section for diagnosing a security of an information system designated by said user, on the basis of diagnosis results in each of said audit sections;

a plurality of management sections for controlling a security status concerning the information security policy of the managed system, each management section being provided so as to correspond to each set of the information security policy and the managed system, which are specified by security specifications hatched by said security specification hatching step, and;

a security handling and management section for

executing a management section designated by said user, to change the security status of the managed system corresponding to the management program so as to adjust the security status to the information security policy corresponding to the management program.